Wide Area Network Backbone	
Subject:	Metro WAN Backbone Standards
Version:	1.0
Author:	Derek Carver
Last Modified:	08/16/2004 1:30 PM

Section I: Revision History

Date	Author	Changes
08/16/2004	Derek Carver	Document creation.

Section II: Table of Contents

Section III: Introduction

The Telecommunications Division of the Information Technology Services (ITS) Department of Metro Nashville is responsible for managing the routers on the County-wide data network. In order to effectively manage these devices, a standardized set of configuration guidelines must be in place. This document will serve as that guideline.

While a guideline is not strictly defined as a set of requirements, it is strongly suggested that all routers installed in the Metro network follow the suggestions in this document. Any required exceptions must be explained and documented in Appendix A of this document.

Section IV: Document Ownership

This document was created and is maintained by the Telecommunications Division of the Information Technology Services (ITS) Department of Metro Nashville and Davidson County. The information in this document is the managed and owned by the Telecommunications Division Manager. Any questions, comments, or requests for further information should be sent to the Telecommunications Division Manager. The Telecommunications Division Manager is Derek Carver (615-880-3813).

Section V: Internetworking Standards

Section V-A: OSI Reference Model

The Open Systems Interconnection (OSI) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for intercomputer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained, so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

The following list details the seven layers of the Open System Interconnection (OSI) reference model:

• Layer 7—Application layer
• Layer 6—Presentation layer
• Layer 5—Session layer
• Layer 4—Transport layer
• Layer 3—Network layer
• Layer 2—Data Link layer
• Layer 1—Physical layer

The focus of the Telecommunications division is primarily on layers 1-3 with a heavy emphasis on layers 2 and 3.
.

Section V-B: TCP/IP

TCP/IP stands for Transmission Control Protocol / Internet Protocol. TCP/IP is a set of protocols (rules) by which most of today's computers communicate with one another and the Internet. Each computer or other network device has an address to differentiate it from the other devices on a network. TCP/IP is the protocol which Metro Nashville Government has adopted as the standard transport protocol used to communicate between logical networks and also the Internet.

Section VI: Network Transport Infrastructure

The Network Transport Infrastructure (NTI) for the Metro Nashville Government was originally engineered and designed as an ATM backbone. There were three ATM aware layer three devices for the entire Metro network. Metro has since upgraded the NTI from ATM to SONET. The advantages of SONET are as follows:

- Eliminates several layers of multiplexing by using synchronous transmission.
- Greater flexibility with a variety of topologies and data rates.
- Standardized optical interfaces (carrier independent)
- Greater versatility based on the flexibility SONET offers

By implementing SONET as the NTI Metro ITS becomes the service provider for the different departments within the Metro Nashville Government. Due to the flexibility of SONET, departments which require private, secure connectivity can be offered the desired solution and have their own private connectivity on the Metro WAN.
SONET technology underlying core transport functions (OC-48, OC-12, OC-3, STS-1, DS-3, and DS-1 interfaces).

Section VII: SONET Backbone

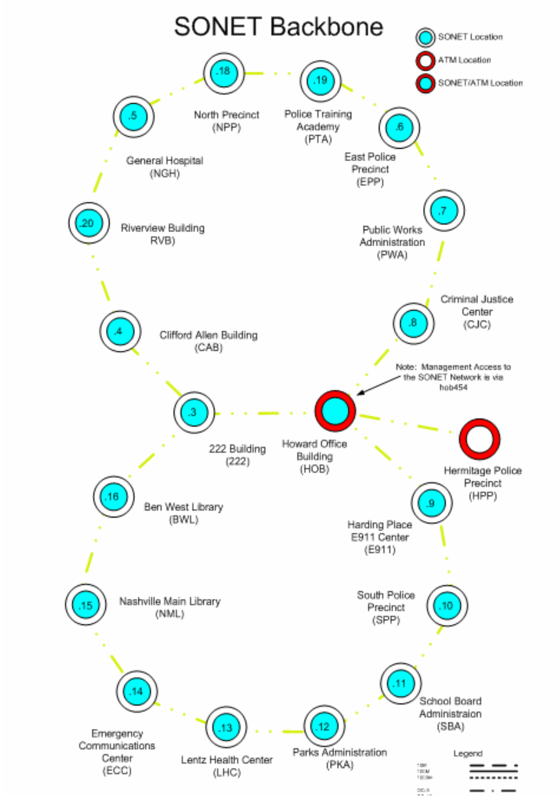
The Metro Nashville Government core backbone consists of 19 Cisco 15454 SONET Multiservice Provisioning Platform. The backbone ring currently is a data rate of OC-48. The SONET ring topology is engineered with UPSR circuits and has a Shared Packet Ring (SPR). The SPR allows for all connected layer 2-3 devices to logically be treated as if they are residing on a local area network. The SONET ring technology allows for redundancy via the ability for the data to traverse the ring in both directions. This allows for sub-50 millisecond recovery time in the case of a fiber break or hardware failure. The follow is a list of SONET carrier speeds available:

- OC-48
- OC-12
- OC-3
- STS-1
- DS-3
- DS-1

The flexibility in the SONET technology also allows for Metro to utilize the ring technology to create telephony PRI circuits across the Metro owned backbone. This offers greater redundancy and cost efficiencies due to the aggregation of PRIs at one or two SONET locations where enterprise PBX solutions have been implemented.

Each SONET platform is provisioned with the following:
2 – OC-48 cards
2 – XCVT cards
1 – Fiber Gigabit Ethernet card
1 – 12 port Copper Ethernet card
1 – OC-3 card
1 – DS-1 card
1 – DS-1N card

Currently there are 19 SONET locations throughout the Metro network. These locations have all been standardized using the Cisco ONS 15454 platform. Existing fiber connections at campus locations have been utilized to offer high speed connectivity to departments and locations within close proximity of a SONET location. The following diagram shows a high level topology of the SONET backbone for Metro.



Section VIII: Wide Area Network (WAN)

Section VIII-A: Hardware Standards

The desire for enterprise wide design for WAN connectivity is to have a layer three device at each building location. The desired design is to have a logical subnetted network at each building location or at a minimum each campus. Depending on the routing need at the SONET backbone location, one of two routers/switches has been designated as the Metro standard for routing at the edge locations. The standardized device is a Cisco Catalyst 3550-12G switch with the enhanced router code. The 3550-12G is utilized for locations which need to accommodate multiple fiber termination points. The 3550-12T is utilized for locations that need gigabit copper uplinks.

Section VIII-B: Routing Protocols

The Metro network uses OSPF as its interior routing protocol. The IP address space assigned to Metro by the American Registry for Internet Numbers (ARIN) is 170.190.0.0/16. That class B network is entirely configured to be in a single OSPF area. Since area 0 (the backbone area) is required to be present in every OSPF network, all of 170.190.0.0/16 is in area 0.

Section IX: Local Area Network (LAN)

Section IX-A: Hardware Standards

The Metro network has standardized on Cisco Catalyst 3550-X or Catalyst 2950 10/100 switches for the access layer switch. This solution offers both high port density per switch and managed stackable switches. The access to the Metro network should be through a switch that is managed by ITS and authentication and authorization for access is performed via the Cisco Secure TACACS+ server. This allows for access to the switches via an Active Directory aware TACACS server. The following diagram shows an example of the Catalyst 3550-48 access switch:

Section IX-B: LAN Protocol Standards

VLANs

The use of VLAN technology is critical to the segmentation and security of the network infrastructure. The Metro standard for VLAN naming is utilizing the third octet of the IP address. If the network IP address is 170.190.23.0/24 then the VLAN that would be defined on the switch would be VLAN_23. All switch ports, save possibly the uplink, would then be assigned to this VLAN and would be configured to function as a separate VLAN from the existing default VLAN1.

Port Configuration

The standard within Metro for port configuration is to hardcode the switch

Section X: Wireless

A Wireless Local Area Network (WLAN) implements a flexible data communication system frequently augmenting rather than replacing a wired LAN within a building or campus. WLANs use radio frequency to transmit and receive data over the air, minimizing the need for wired connections.

Section X-A: Wireless Policy Statements

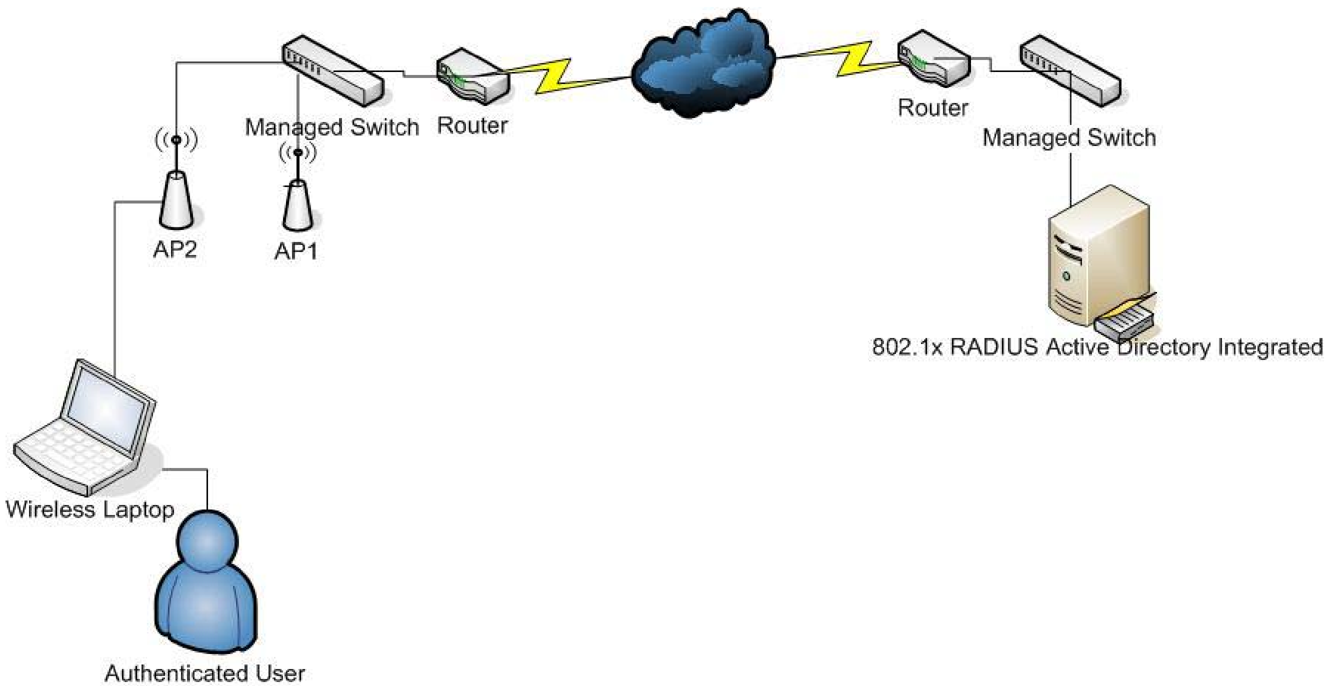
- All wireless networking equipment will conform to the specifications developed by the Institute of Electrical and Electronic Engineers. (IEEE)
- Any wireless networking equipment currently deployed prior to the acceptance of the wireless standard that does not meet the security specifications defined in the wireless standards document is subject to removal.
- Access to wireless services will be restricted to authorized users only.
- Wireless networking equipment shall not be installed on the Metro network without consent and approval from ITS Telecommunications Division.
- Requests for wireless service can be made by contacting the MNPS NSG.
- Violation of the End User Computer Agreement policy can result in the revocation of authorization to use all network services.

Section X-B: Hardware Requirements

- Wireless Access Points
  - Operate in the 2.4 GHz frequency range. (802.11b/g)
  - Standard and proprietary alarms for notification of device status and events (SNMP)
  - Secure remote management
  - Power over Ethernet PoE (802.3af)
  - RADIUS authentication (802.1x)
  - VLAN (802.1Q)
  - 64, 128, and 152 bit WEP
  - Rouge access point detection and notification
  - Wi-Fi Certified
- Wireless Network Interface Card
  - Form Factor: CardBus Type II, PCI Card 32 bit
  - Data Rates: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
  - Network Standard: IEEE 802.11b/g
  - Media Access Protocol: Carrier-sense multiple access w/Collision Avoidance
  - OS: Windows 2000, XP

Section X-C: LAN Wireless Security

The proposed method of securing the MNPS WLAN will be a combination of 802.1x RADIUS in conjunction with the existing network Active Directory Services currently in place. Central management and rouge access point detection will be provided by Metro ITS Telecommunications Division.



Section XI: Guidelines for WAN/LAN Equipment

The Telecommunications Division has standardized on Cisco routers for use within Metro's networks. All configuration examples are taken from Cisco router configurations.

The guidelines in this document apply to the following router configuration areas:

- Device naming
- Security
- Name resolution
- Time synchronization
- SNMP variables
- IP forwarding
- Loopback interfaces
- OSPF configuration
- Cisco-specific configuration

Section XI-A: Device naming

All devices management by the Telecommunications Division comply with the ITS Naming Standard. The naming standard is published in the Exchange Public

Folders. In addition to the device name, all interfaces on a router must have an entry in the internal DNS (in the net.nashville.org subdomain). Interface naming follows the following format:

aaart**bb**-**ccc**-tr**dd**

Where:

aaa is a three-letter location ID as described in the ITS Naming Standard;
rt is a two-letter device ID as described in the ITS Naming Standard;
bb is a two-letter device ID;
ccc is a variable-length interface name as described below;
tr stands for "Telecommunications Room";
dd is a variable-length identifier for the location of the device within the building as described below.

An example of a router interface name would be:

`hobrt08-fa0-2-tr0c9`

Where:

hob designates that the device is located within the Howard Office Building;
rt designates that the device is a router;
08 designates that this is the 8th router installed at Howard Office Building;
fa0-2 designates that the router interface is FastEthernet0/2;
tr0c9 designates that the router is installed in the 9th rack in the basement comm room at HOB.

Each interface on a router must have an entry in the internal DNS in the net.nashville.org subdomain. Additionally, a CNAME must be entered for the router's short name, pointing to the management interface[1]. The following example illustrates the DNS entries that may be created for a router:

Entry	Type	Data	Description
hobrt08-fa0-2-tr0c9	A	10.1.1.3	Interface FastEthernet0/2
hobrt08-fa0-0-tr0c9	A	10.1.2.3	Interface FastEthernet0/0
hobrt08-s2-tr0c9	A	10.1.3.3	Interface Serial2
hobrt08-lo0-tr0c9	A	10.1.4.3	The loopback interface
hobrt08	CNAME	hobrt08-lo0-tr0c9	The alias for the router's short name

[1] The management interface on a router is preferably the loopback interface.

Please contact the DNS administrator for the net.nashville.org domain to have the entries added when a router is installed, or whenever the IP address of an interface changes.

The router's short name is configured as the hostname within the configuration. On a Cisco router, this is configured using the following command:

```
hostname [Router short name]
```

Section XI-B: Security

Since the routers on the Metro network carry mission critical data, they must be protected from unauthorized changes to configurations. The routers are managed through telnet, SNMP and/or web access. Each area must be secured.

- **Telnet**

Telnet access to routers is authenticated through a centralized TACACS+ server. As a backup in the case of a failure of the TACACS+ server, a local username and enable secret is configured as well. To set up TACACS+, contact the TACACS+ administrator to have the loopback address of a new router added to the TACACS+ server. The following commands configure a router for secure telnet access:

```
enable secret [omitted]
username [omitted] privilege 15 password [omitted]
line vty 0 4
 password [omitted]
ip tacacs source-interface Loopback0
tacacs-server host 170.190.6.45
tacacs-server directed-request
tacacs-server key [omitted]
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication ppp default group tacacs+ local
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 engineering group tacacs+
aaa authorization network default group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
```

- **SNMP**

The SNMP community strings for read-only access and read-write access must be configured on a router. The following commands configure the community strings:

```
snmp-server community [omitted] RO
snmp-server community [omitted] RW
```

Additional SNMP settings should also be configured and are explained later in this document.

- **Web**

Security for the web interface on a Cisco router is included in the configuration example for Telnet, which is outlined earlier in this document.

Section XI-C: Name resolution

All routers should be configured for name resolution through internal DNS servers. The commands for configuring name resolution are as follows:

```
ip domain-name net.nashville.org
ip name-server 170.190.6.196 170.190.128.221
```

Section XI-D: Time synchronization

All routers should have their time synchronized through NTP or SNTP – whichever the router supports. The configuration commands are similar and are shown below.

- **NTP**

```
ntp source Loopback0
ntp server 170.190.2.1
ntp server 170.190.2.2
```

- **SNTP**

```
sntp server 170.190.2.1
sntp server 170.190.2.2
```

For the time to display accurately, it is recommended that routers are configured with the correct timezone settings. This is done with the following commands:

```
clock timezone CST -6
clock summer-time CDT recurring
```

Section XI-E: SNMP Variables

In addition to the community strings explained earlier in this document, the location and contact SNMP variables should always be configured.

The location variable should be set to explain in plain English the location of the router. This can be configured using the command in the following example:

```
snmp-server location Howard Office basement comm rm rack 9
```

The contact variable should be exactly the same on every piece of network equipment. The configuration follows:

```
snmp-server contact Metro ITS 615-862-6300
```

Section XI-F: IP forwarding

IP forwarding is used to forward DHCP broadcasts to a DHCP server on a remote network. On a Cisco router, this is configured in the interface configuration using the “ip helper-address” command. The issue with IP forwarding is that when it is turned on, the default action is to forward a number of different types of broadcast packets in addition to DHCP. Therefore, every router should be configured to exclude any types of broadcast forwarding except for DHCP. This can be configured using the following commands:

```
no ip forward-protocol udp tftp
no ip forward-protocol udp domain
no ip forward-protocol udp time
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
no ip forward-protocol udp tacacs
```

Section XI-G: Loopback interfaces

Loopback addresses are virtual interfaces which can be included in a dynamic routing protocol. They allow a router to be remotely accessed any time at least one physical interface is functional and is participating in dynamic routing. On the Metro network, the 170.190.2.0/24 address ranged has been reserved for loopback addresses. Each loopback address is configured with a thirty-two bit subnet mask (255.255.255.255) and must be included in the OSPF routing process. A loopback interface can be configured using the following example commands:

```
interface loopback0
ip address 170.190.2.240 255.255.255.255
no shutdown
```

Again, the interface must also be included in the OSPF configuration. This is generally accomplished by placing the entire 170.190.0.0/16 network in area 0 using the following command:

```
router ospf 1
 network 170.190.0.0 0.0.255.255 area 0
```

Section XI-H: OSPF configuration

The Metro network uses OSPF as its interior routing protocol. The IP address space assigned to Metro by the American Registry for Internet Numbers (ARIN) is 170.190.0.0/16. That class B network is entirely configured to be in a single OSPF area. Since area 0 (the backbone area) is required to be present in every OSPF network, all of 170.190.0.0/16 is in area 0. This is configured on a Cisco router using the following command:

```
router ospf 1
 network 170.190.0.0 0.0.255.255 area 0
```

Section XI-I: Cisco-specific configuration

Some recommended configuration settings are unique to Cisco routers. These include:

- Debug and logging timestamps
- Password encryption
- Interface descriptions
- VTY passwords

They are outlined in the following sections.

Debug and logging timestamps

By default, debugging and logging messages are stamped with the elapsed time since the router was booted instead of the actual date and time. This can be changed using the following commands:

```
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
```

Password encryption

The passwords stored in a Cisco router configuration are stored as plain text by default. The following command will store them using a rudimentary encryption algorithm:

```
service password-encryption
```

Interface descriptions

Where possible, all interfaces should have descriptions configured. These should state in plain English the purpose of the interface, including the remote destination of point-to-point interfaces. The following example illustrates the commands for configuring an interface description:

```
interface Serial0/0
 description T1 to hobrt08, interface Serial1
```

VTY passwords

During the initial configuration of a router, there is no password configured by default on the vty lines. If the TACACS+ configuration is not working and there is no password on the vty lines, no one will be able to log in to the router through telnet. Therefore, it is very important to set a password on the vty lines. This is done through the following command:

```
line vty 0 4
 password [omitted]
```

Section XII: Conclusion

All routers installed on the Metro network should be configured according to a standard set of guidelines. This will facilitate ease of management, efficient network support, and the implementation of new network management systems. This document contains the router configuration guidelines to be used on Metro routers.

Any questions regarding the information in this document should be forwarded to the Telecommunications Division Manager.